Nuts and Bits of PKI

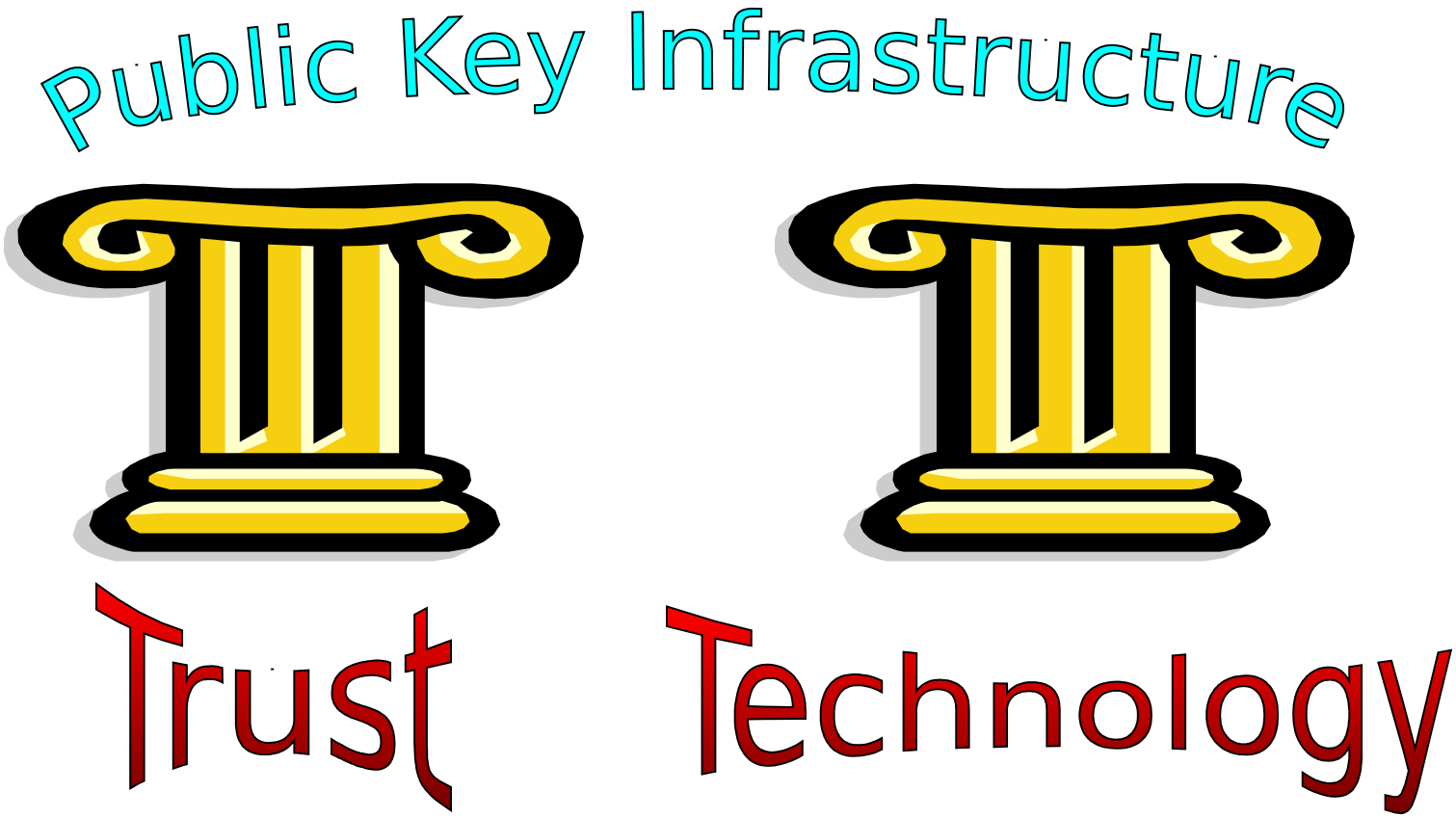
Mark L. Silverman, CISSP

Center for Information Technology

National Institutes of Health

CENDI Symposium on PKI and Digital Signatures
June 13, 2001

Foundations of PKI



Start with Technology

- Cryptography
  - Basic (single key) cryptography
  - Public (dual) key cryptography
- Digital Signatures

Conclude with Trust

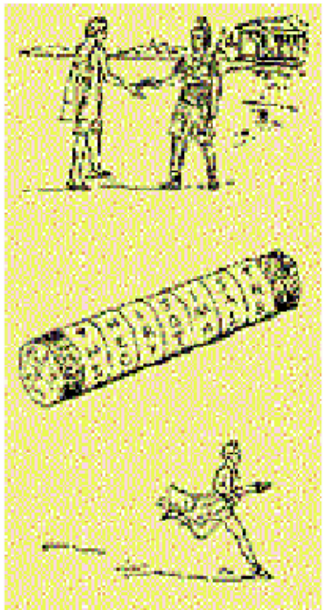
- Digital Certificates
- PKI Authorities
  - Policies
- Trust beyond the enterprise
  - Trust paths
  - Bridge PKI Architecture

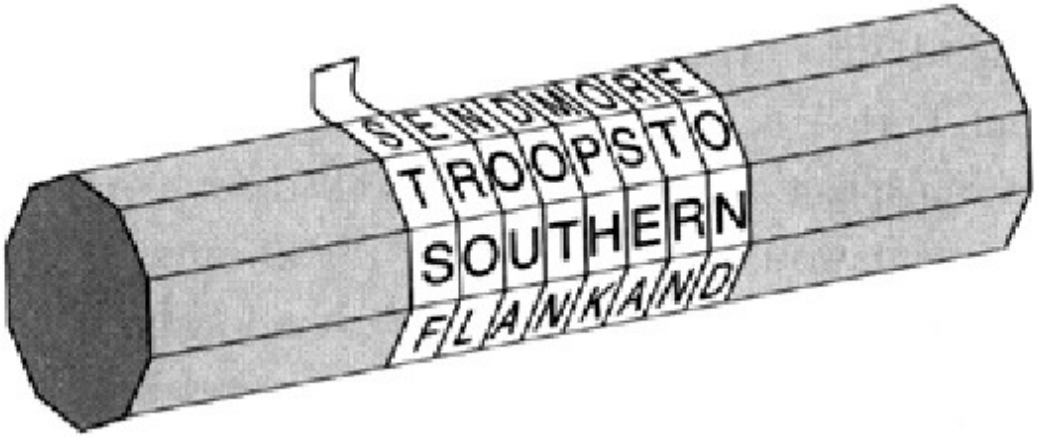
Cryptography

- Science of secret (hidden) writing
  - kryptos – hidden
  - graphen –to write
- Encrypt / encipher
  - Convert plaintext into ciphertext
- Decrypt / decipher
  - Convert ciphertext into plaintext

Spartan Scytale

- Oldest known cryptographic device
  - Fifth century B.C.





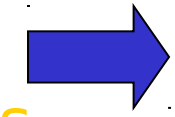
Caesar Cipher

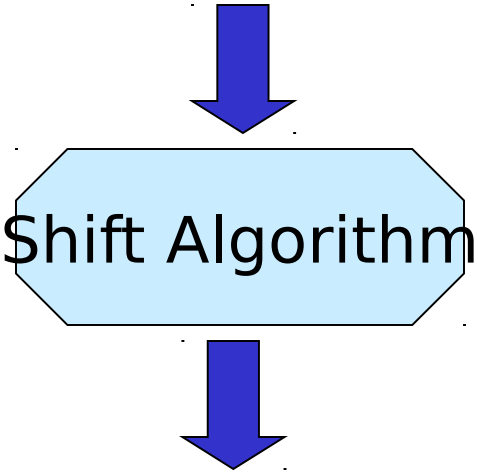
- Julius Caesar, 49 BC
  - Securely communicate with friends
- Simple substitution cipher
  - Shift alphabet 3 characters

Caesar Cipher Example

Plaintext: **ET TU BRUTE**

3 characters





Ciphertext: **HW WX EUXWH**

Symmetric Encryption

- Single key
  - *Shared secret*
- Examples
  - Data Encryption Standard (DES)
    - Block Cipher, 56 bit key
    - Triple DES 112 bit key
  - Advanced Encryption Standard (AES)
    - Rijndael Algorithm
      - Belgian cryptographers, Joan Daemen and Vincent Rijmen.
    - 128, 192, 256 bit keys

Symmetric Encryption Example

Alice

Bob

Dear Bob:

How about coming over to my place at 1:30? If Ted ever finds out we are meeting like this it could be disastrous.

Love, Alice

encrypt

ciphertext

011100111001001
110011100111001
001110000111111

decrypt

Dear Bob:

How about coming over to my place at 1:30? If Ted ever finds out we are meeting like this it could be disastrous.

Love, Alice

Symmetric Encryption Issues

- Key (shared secret) vulnerable to discovery
- Need to share a unique secret key with each party that you wish to securely communicate
  - Key management becomes unmanageable

Asymmetric Encryption

- Two mathematically related keys
  - Unable to derive one from the other
  - Encrypt with one – decrypt with other
- Public Key Cryptography
  - One (public) key published for all to see
  - Other (private) key kept secret
- Algorithms
  - RSA - Integer Factorization (large primes)
  - Diffie-Hellman - Discrete Logarithms
  - ECES - Elliptic Curve Discrete Logarithm

Asymmetric Encryption Example

Ted

Carol's Public Key

Carol's Private Key

Carol

Dear Carol:

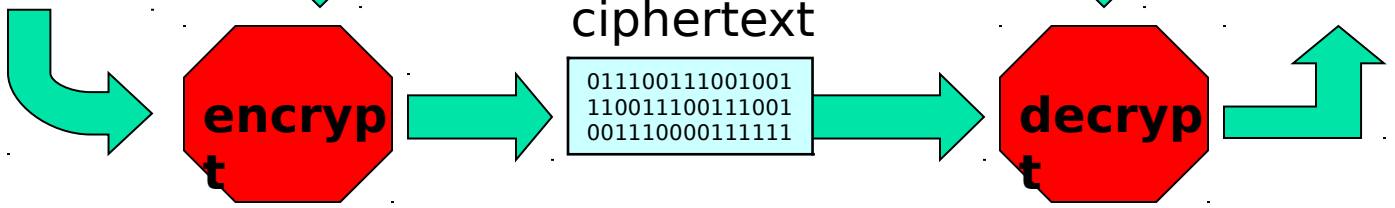
I think Alice is having an affair with Bob. I need to see you right always.

Love, Ted

Dear Carol:

I think Alice is having an affair with Bob. I need to see you right always.

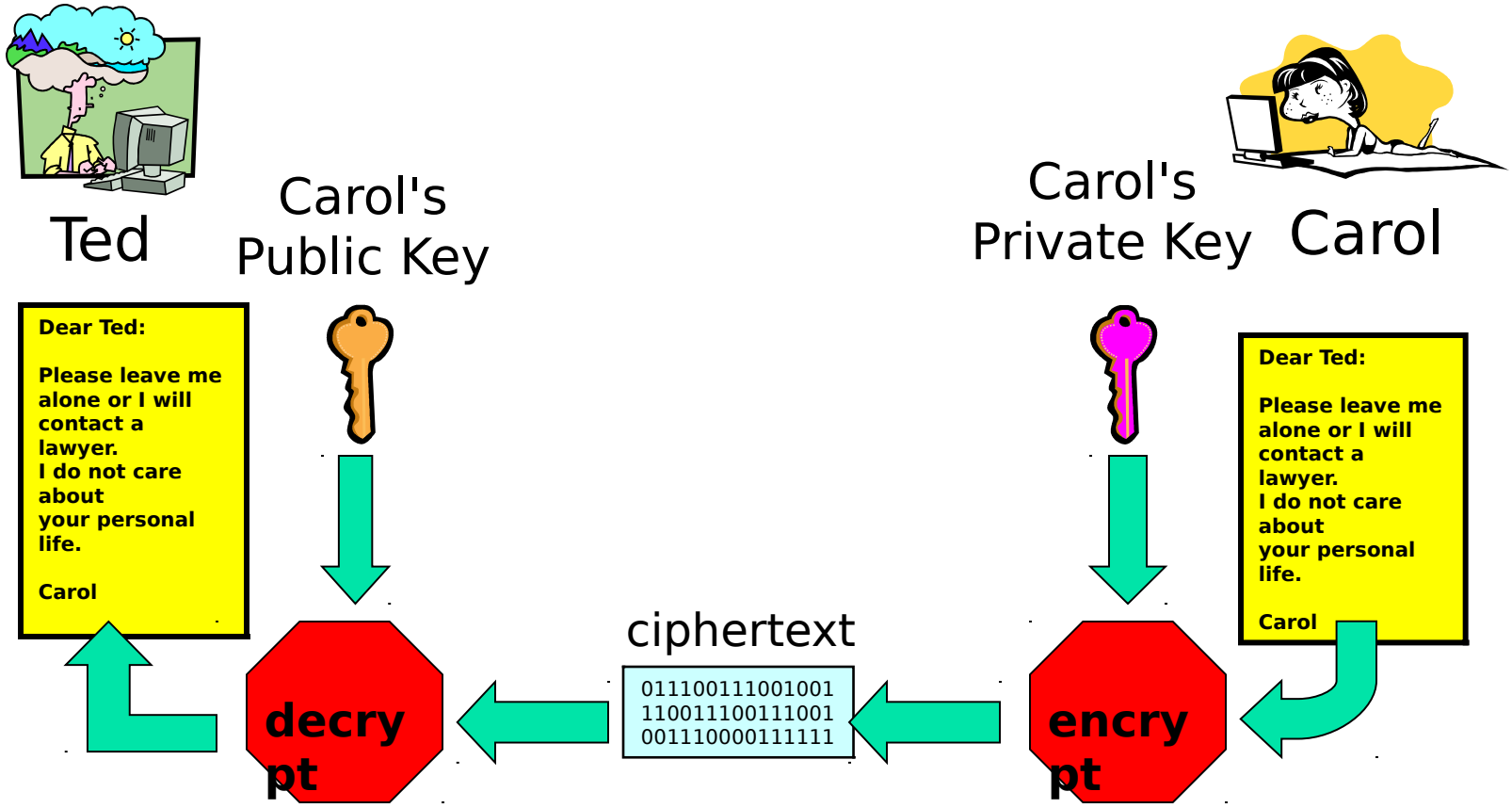
Love, Ted



Asymmetric Advantages

- No shared secret key
- Public key is public
  - Can be freely distributed or published
  - Key management is much easier
- Private key known ONLY to owner
  - Less vulnerable, easier to keep secret
- Supports Non-repudiation
  - Sender can not deny sending message

Asymmetric Non-Repudiation



Non-repudiation

- Since only the sender knows their private key, only the sender could have sent the message.
- Authentication mechanism
- Basis for Digital Signature

Asymmetric Issues

- More computationally intensive
  - 100x symmetric encryption
- Generally not used to encrypt data
  - Encrypt symmetric key (S/MIME)
  - SSL session key

SMIME Encryption

Dear Carol:

Please do not push me away.
I love you more than I do
Alice.

Love, Ted

encrypt

A032F17634
E57BC43356
743212b9c9
8FA2917342
5633A22201
807732ECF1
3344567520
ABCE4567CD

0111001110
1100111001
0011100001

decrypt

Dear Carol:

Please do not push me away.
I love you more than I do
Alice.

Love, Ted

encrypt

decrypt

Carol's Public Key

Carol's Private Key

Electronic Signatures

Electronic Signature != Digital Signature

Electronic Signatures in Global and National Commerce Act (E-Sign) defines:

The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

Digital Signature

- Type of Electronic Signature
- Combines one-way secure hash functions with public key cryptography
  - Hash function generates fixed length value
  - No two documents produce the same hash value
  - Secure Hash Algorithm 1 (SHA-1)
- Characteristics
  - Data Integrity - hash value
  - Non-repudiation – encrypted with private key
  - Does NOT provide confidentiality

Digital Signature Creation

Sue

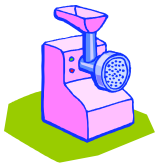
Dear Mr. Ted:

We have asked the Court to issue a restraining order against you to stay away from Carol.

Sincerely,

Sue Yew
Dewey, Cheatam & Howe, Law Firm

Sue's Private Key



Hash Function

Hash Value

0F47CEFF
AE0317DB
AA567C29

encrypt

Dear Mr. Ted:

We have asked the Court to issue a restraining order against you to stay away from Carol.

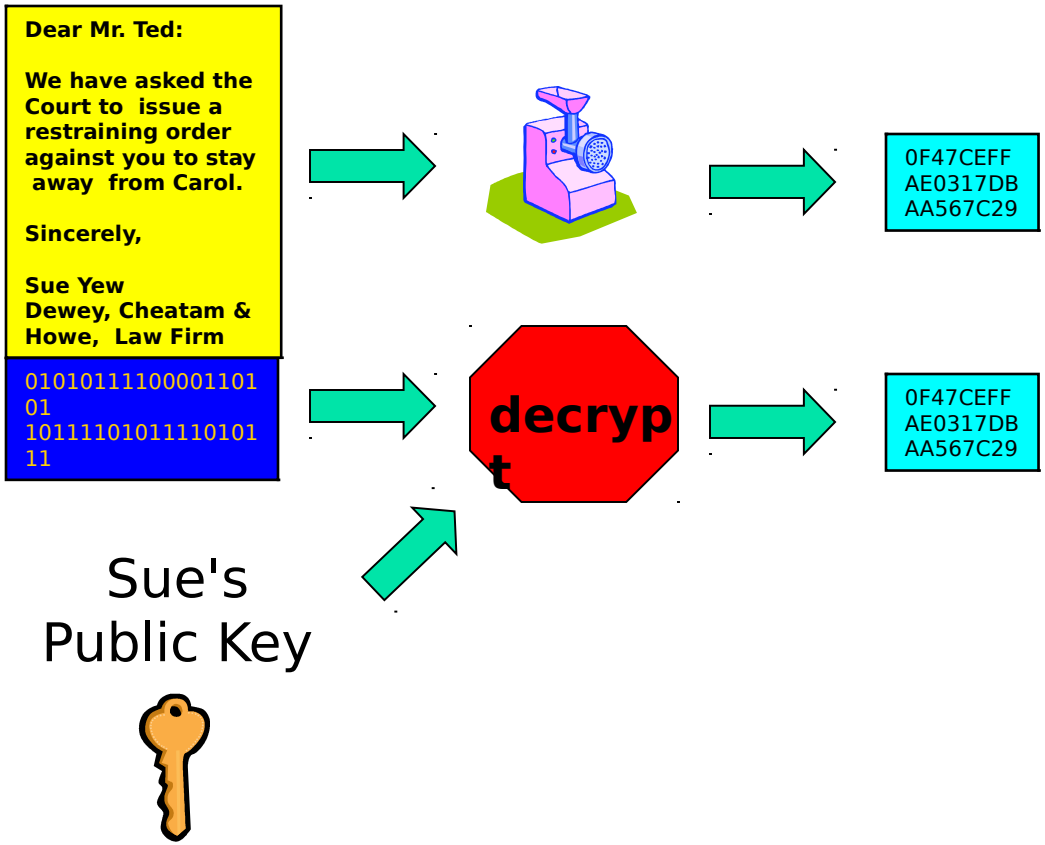
Sincerely,

Sue Yew
Dewey, Cheatam & Howe, Law Firm

01010111100001101
01
10111101011110101
11

Digital Signature

Digital Signature Validation


Dear Mr. Ted:
We have asked the Court to issue a restraining order against you to stay away from Carol.
Sincerely,
Sue Yew
Dewey, Cheatam & Howe, Law Firm
01010111100001101011111010111101011111
0F47CEFF AE0317DB AA567C29
decrypt
0F47CEFF AE0317DB AA567C29
Sue's Public Key

Signature is valid if the two hashes match

Source of Public Key

- Keys can be published anywhere
- Attached as a signature to e-mail
  - Pretty Good Privacy (PGP)

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 7.0.4

iQCVAwUBOx6SgoFNSxzKNZKFAQGK+gP6AnCVghZqbL3+rM5JMSqoC5OEYIkbvYZN
92CL+YSCj/EkdZnjxFmU9+wGsWiCwxvs/TzSX6SZxlpG1bHFKf0OPu7+JEfJ7J5z
cPCSqbFXiXzmukMl5KNx0p0veIDW4DmwleDpkmhT05qnCheweoNyvTSzfA1TGeLl
mpjBi6zUjiY=
=Xq10
-----END PGP SIGNATURE-----
```

But

- How do you know for sure who is the owner of a public key?

Public Key Infrastructure

Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. NIST

The set of hardware, software, people, policies and procedures needed to create, manage, sto distribute, and revoke Public Key Certificates b on public-key cryptography. IETF PKIX working gro

Public Key Certificates

- Digital Certificates
  - Binds a public key to it's owner
  - Issued and digitally signed by a *trusted* third party
  - Like an electronic photo-id
- Follows X509 V3 standard – RFC 2459

X509 V3 Basic Fields

- Owner's X.500 distinguished name (DN)
  - C=US;O=GOV;O=NIH;OU=CIT;CN=Mark Silverman
- Owner's public key
- Validity period
- Issuer's X.500 distinguished name

X509 V3 Extensions

- Location of certificate status information
- Location of Issuer's certificate
- Subject's Alternative Name
  - email address, employee ID
- Key Usage constraints
  - Only for digital signatures
  - Only for encryption
- Policy information
  - Level of trust

X509 V3 Certificate

Version	2 (V1=0, V2=1, V3=2)
Serial Number	56
Signature Algorithm	sh1RSA
Issuer DN	C=US;S=UTAH;O=DST;OU=DSTCA;CN=RootCA
Validity Period	05/02/2000 08:00:00 to 05/02/2001 08:00:00
Subject DN	C=US;O=GOV;O=NIH;OU=CIT;CN=Mark Silverman
Subject Public Key	RSA, 3081 8902 8181 ... 0001
Issuer UID	Usually omitted
Subject UID	Usually omitted
Extensions	Optional Extensions
Signature	sh1RSA (same as above)

PKI Components

- Certification Authority (CA)
- Registration Authority (RA)
- Repository
- Archive
- Users

Certification Authority (CA)

- TRUSTED third party
- Issues Certificates
  - Creates and signs them
  - Publishes current certificates
- Issues Certificate Revocation Lists (CRLs)
  - List of invalid (revoked) certificates
  - Online Certificate Status Protocol (OCSP)
- Maintains archives of status information
- May retain copy of data encryption private key, for purposes of key recovery
  - government requirement

Registration Authority (RA)

- Verify certificate contents for CA
  - Identity proofing
  - RA's public key known to CA
- A CA may have multiple RAs

Repository

- Directory
  - Critical component of a PKI
  - Lightweight Directory Access Protocol (LDAP)
- Stores and distributes
  - Certificates
  - CRLs
  - Other PKI information and policies
- Does not need to be trusted
  - Certificates & CRLs signed by CA

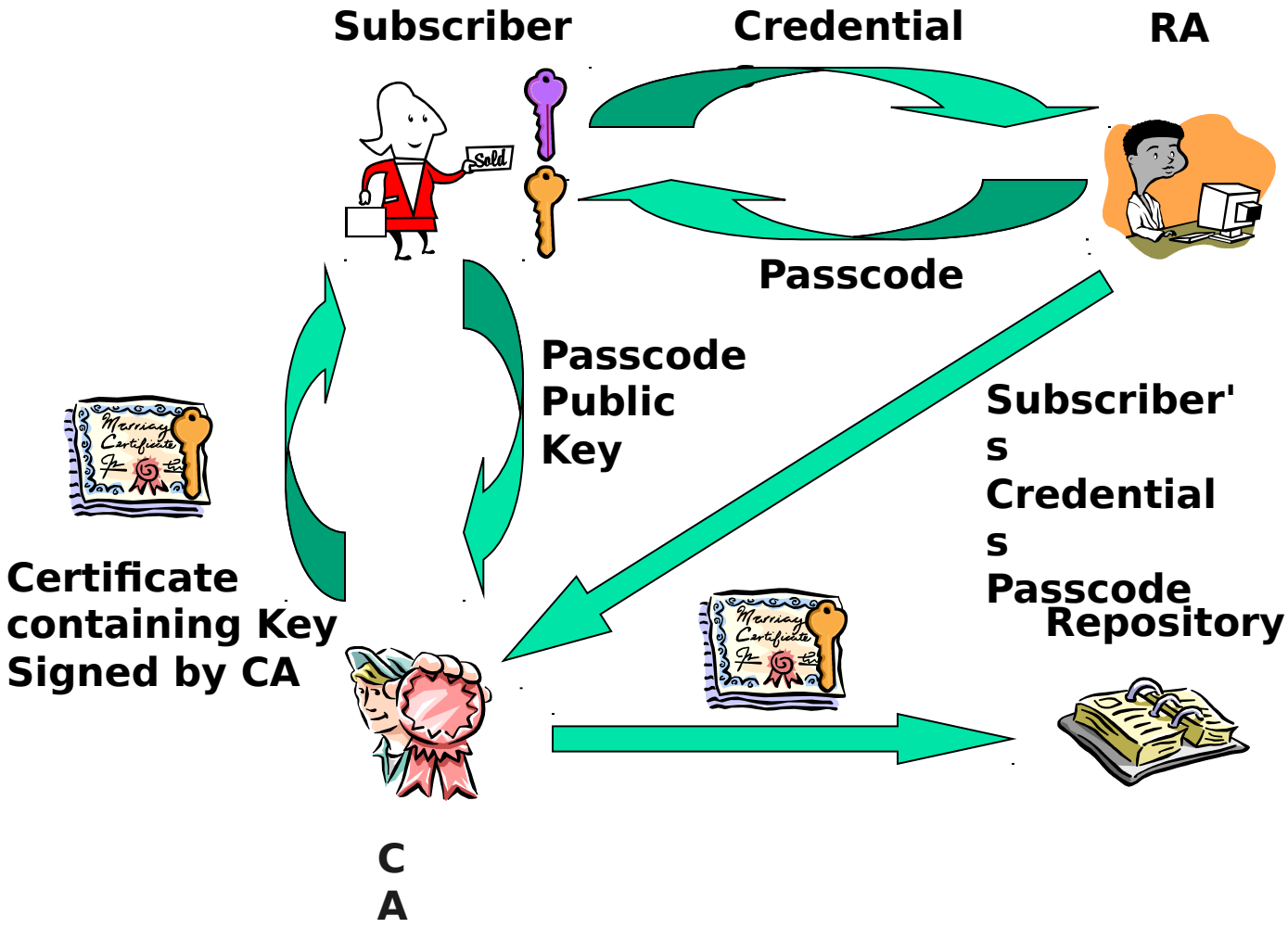
Archive

- Long-term storage on behalf of CA
- Permits verification of old signatures
  - proof signature was valid at time of signing

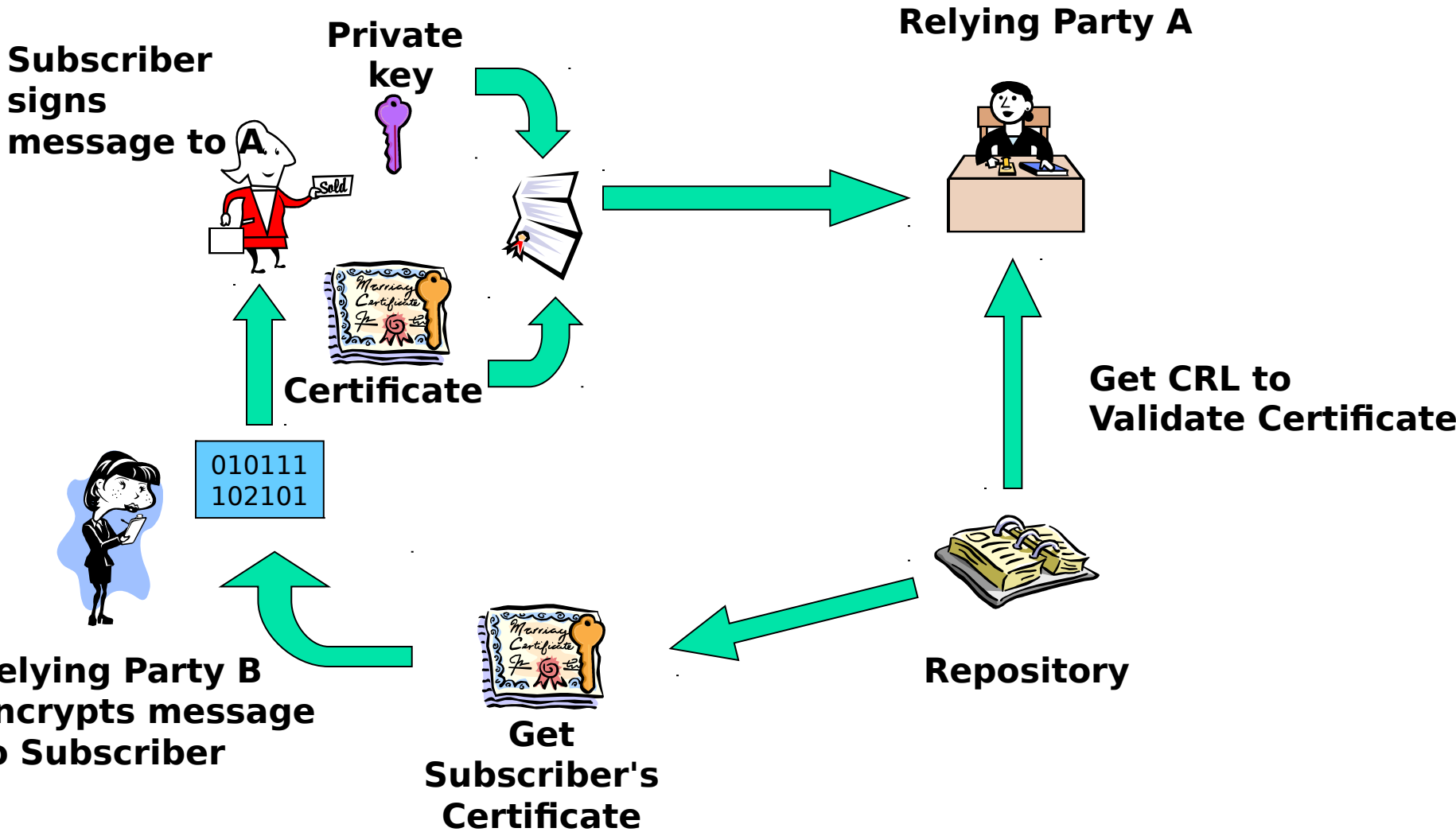
Users

- Subscriber
  - Certificate holder
  - Person, device, application, etc.
  - Non-repudiation requires only subscriber has access to private key
    - Strong identity proofing
    - Owner must protect private key
      - Safer with hardware token / smart card
      - Best security with biometric component
- Relying Party
  - Certificate recipient

How a PKI Issues Certificates



How Certificates are used



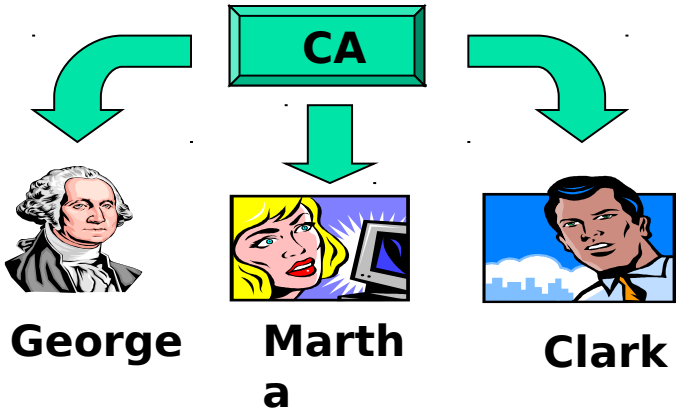
Trusted Third Party

PKI is built upon the concept of the trusted third party (i.e., CA)

But, who are you going to trust?

Who do you Trust?

- Everyone trusts their CA
  - Trust all certificates issued by their CA



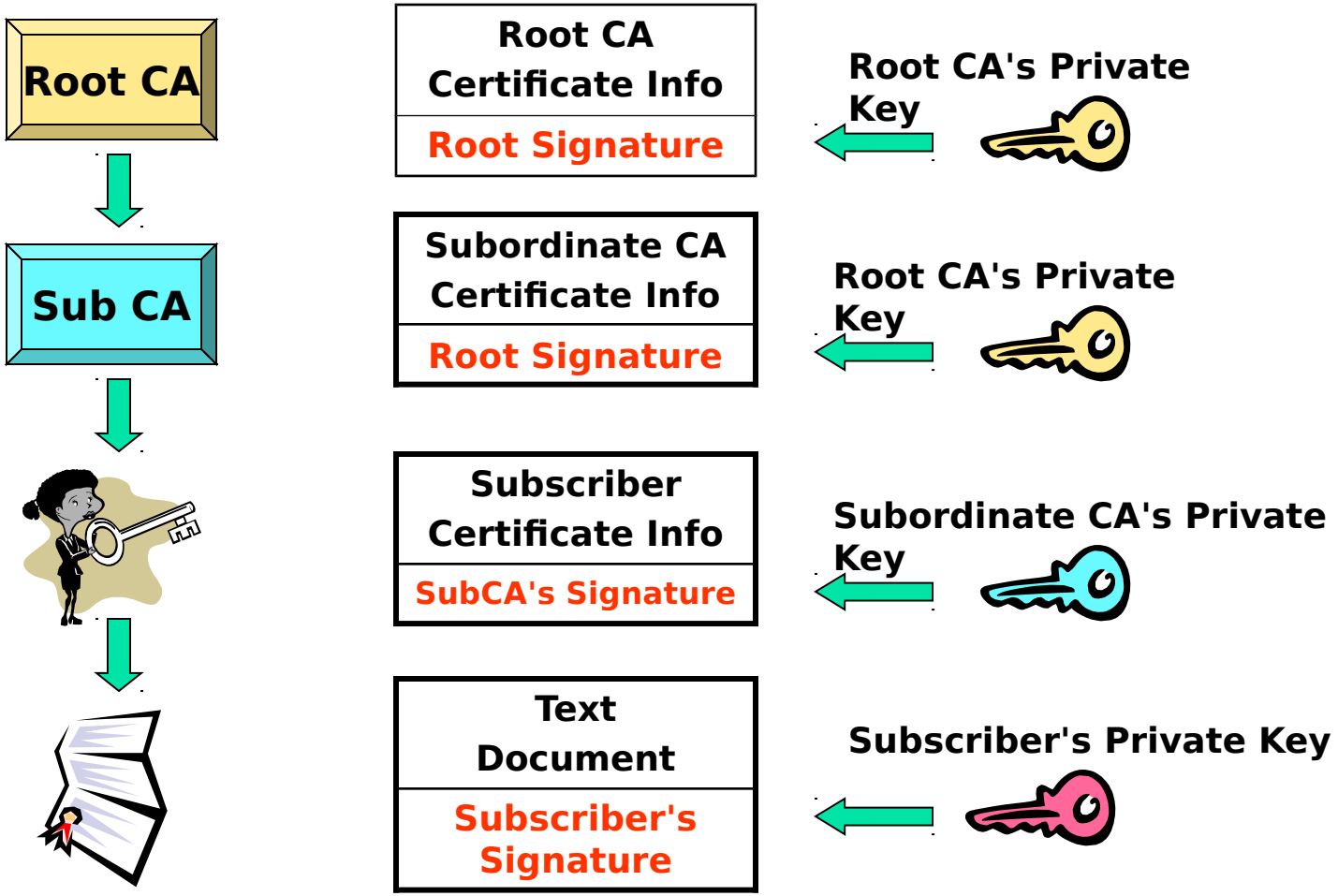
- Single CA model does not scale well
  - Difficult to manage across large or diverse user communities

Hierarchical PKI

- Traditional PKI model is hierarchical
  - CAs have superior-subordinate relationships
  - Higher level CAs issue certificates to subordinate CAs
    - They issue certs to other CAs or end-entities (subscribers)
  - Everyone *trusts* top-level (root) CA
- Forms a certification path
  - Chain of certificates from trust point (root) to end entity (subscriber)

Certification Path

Self Signed



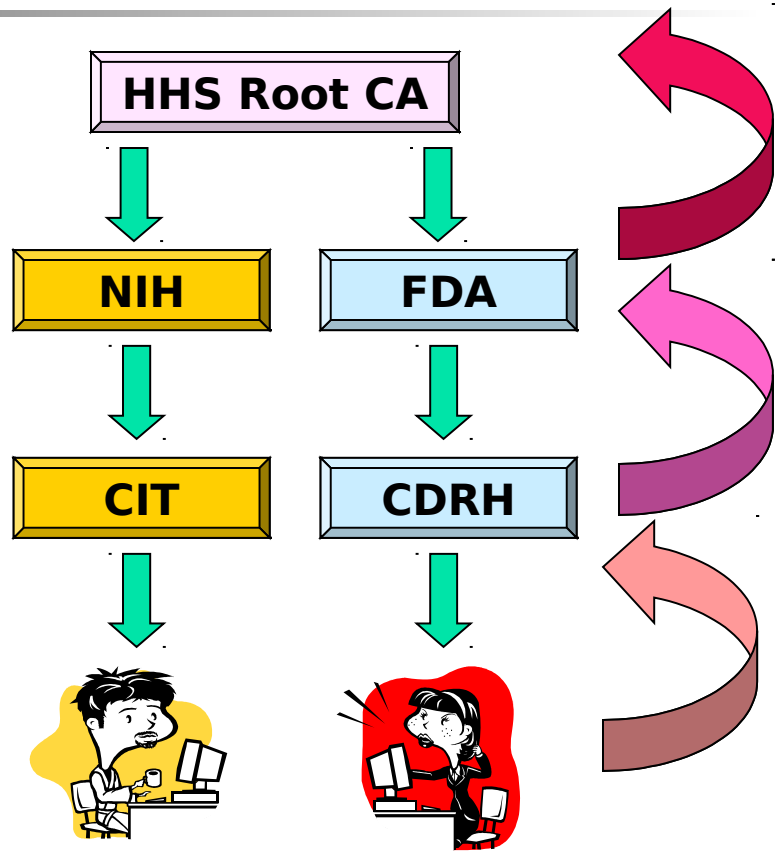
Building a Certification Path

Certification paths are constructed from the end-entity to a trust point

Mark gets cert from Phyllis

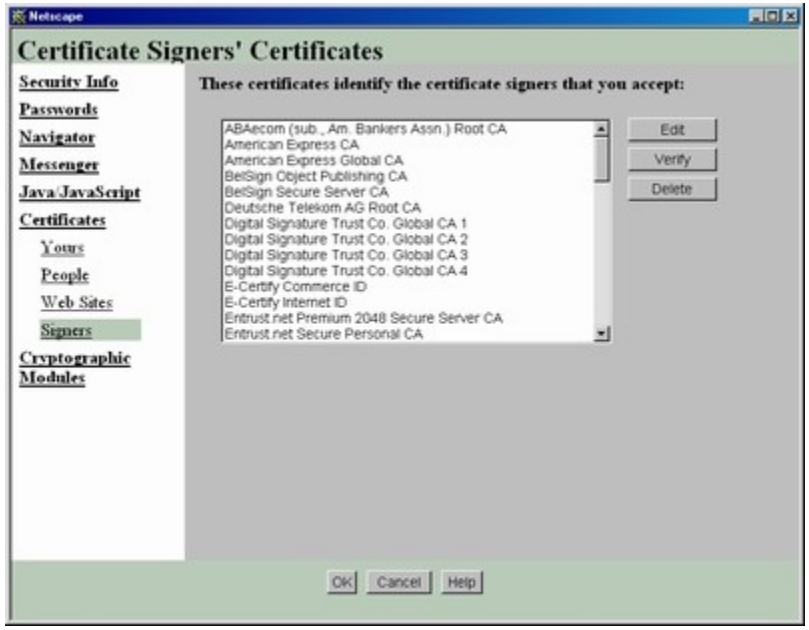
1. Phyllis's cert signed by CDRH
2. CDRH's cert signed by FDA
3. FDA's cert signed by HHS

HHS is Mark's trust point, therefore Mark trust's Phyllis's cert



What about other CAs?

- Trust list: list of CA's trusted by user
  - Commercial CAs often pre-loaded
  - Maintained by user

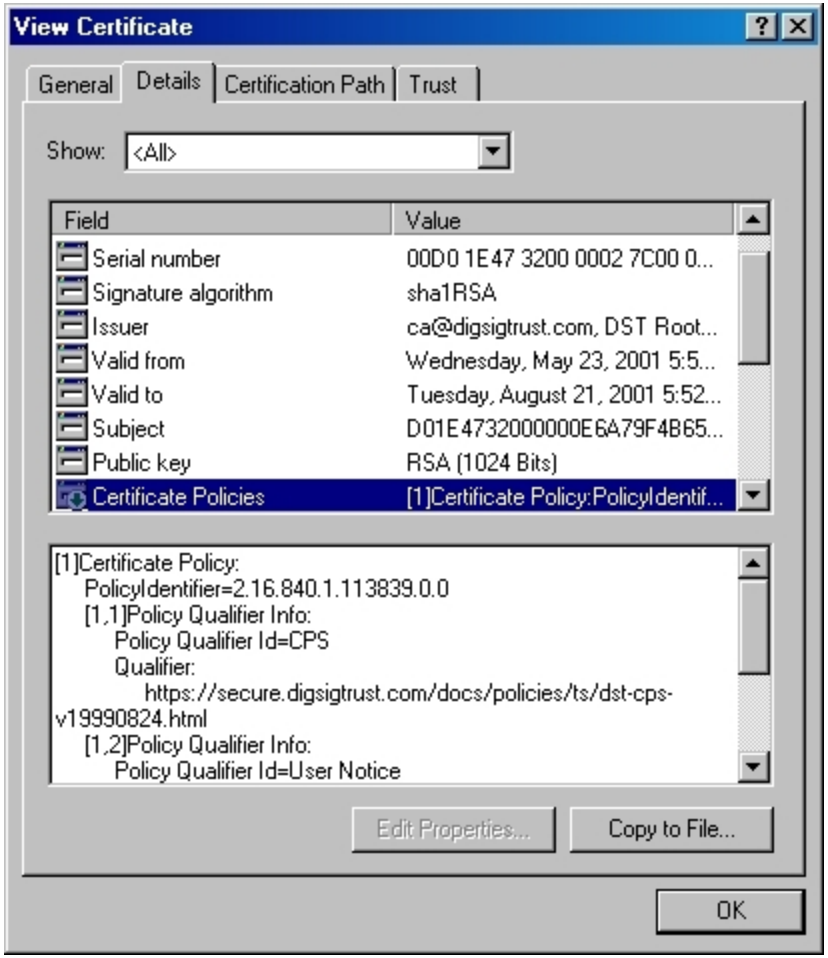


CAs not on the Trust List?

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate matches the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

How do you know if you can trust the CA

Policies



- Policy information contained in
  - CA's Certificate Policy
  - CA's Certification Practices Statement

Certificate Policy (CP)

- A high level document that describes the security policy for issuing certificates and maintaining certificate status information.
- Describes operation of the CA.
- Defines user's responsibilities for requesting, using and handling certificates and keys.

Certification Practice Statements (CPS)

- A highly detailed document that describes how a CA implements a specific CP.
- Specifies the mechanisms and procedures that are used to achieve the security policy.
- Effectively the CA's operations manual.

Policy Issues

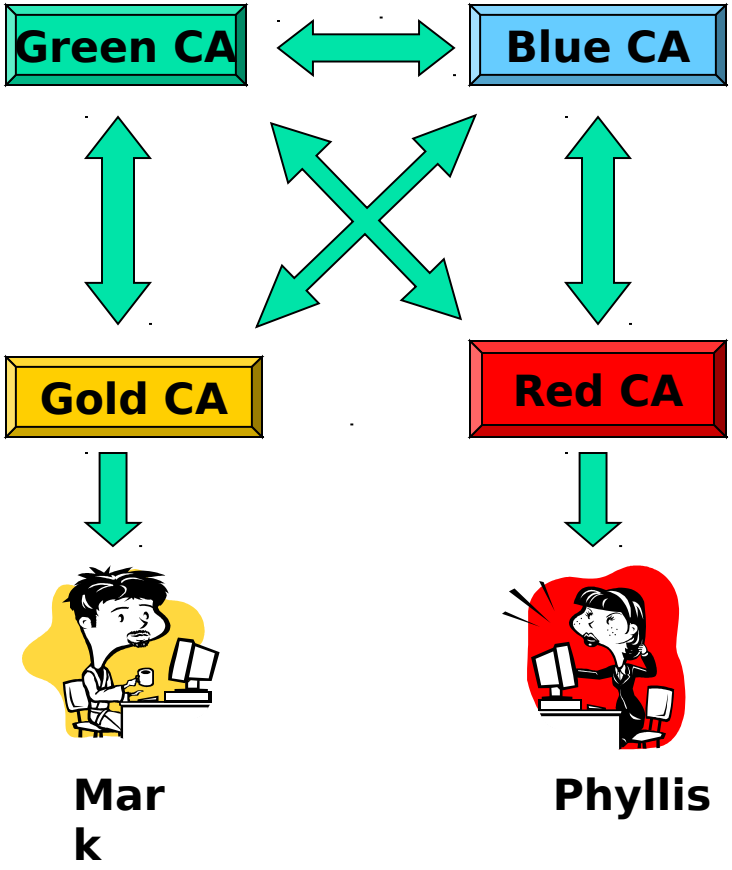
- Users generally don't examine policies
  - Add CAs to trust list out of expediency
  - Don't know status of CA
    - Any policy changes?
    - Was it compromised?

Cross-Certified PKIs

- Peer-to-peer trust relationship
  - Between CAs or hierarchical PKI root CAs
- CAs issue certificates to each other
- CAs review each other's policies
  - Policy mapping
    - Translates policy information
    - A's class 3 certificate = B's medium certificate

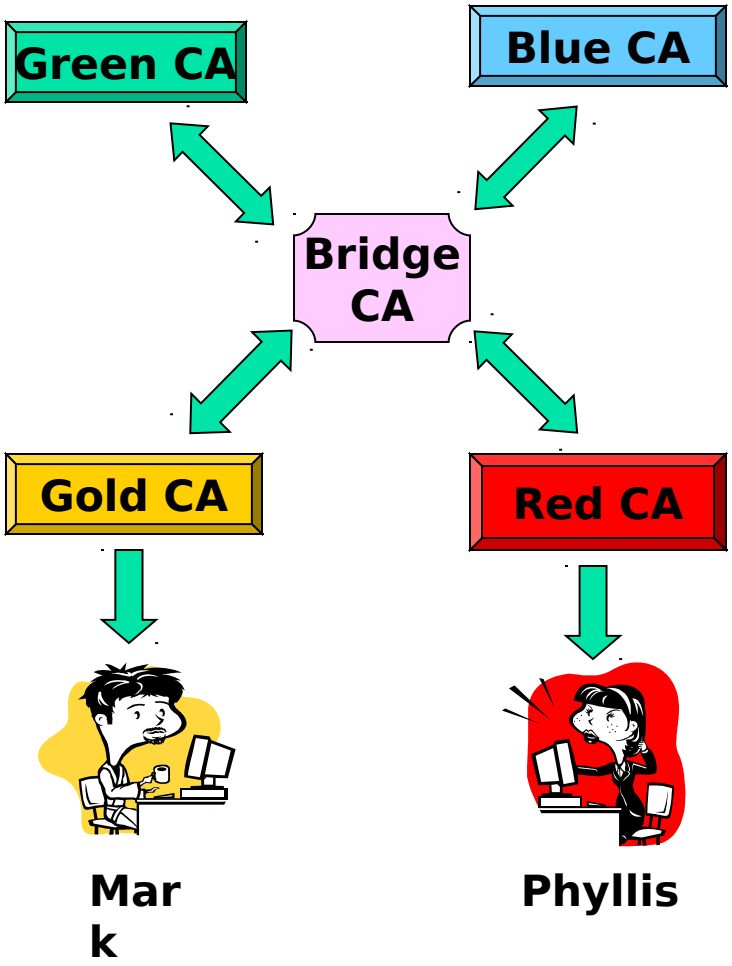
Mesh PKI Architecture

- Advantages
  - CAs are organizationally independent
    - Have independent policies
  - CA compromise does not effect others
- Disadvantages
  - Hard to build certification path
    - Multiple possible paths
    - Loops and dead ends
  - CA needs to maintain multiple relationships with other CAs



Bridge PKI Architecture

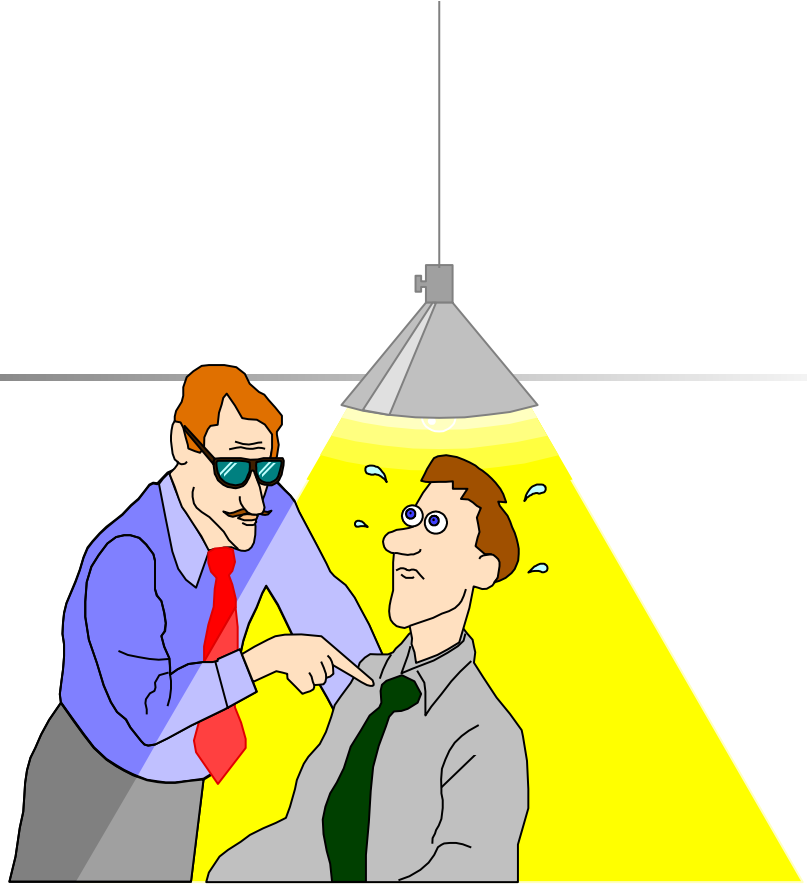
- Bridge is trust arbitrator
  - Only cross-certifies with other CAs
  - Relationships still peer-to-peer
    - Bridge is NOT a root CA
- Certification path construction is much easier
- Bridge does all policy management
  - Less work for the CAs
  - Maintains list of revoked CAs (CARL)



Conclusion

- Enabling technology for E-Gov
  - Data Confidentiality
  - Data Integrity
  - Non-repudiation
- Technology is complicated
  - But not unmanageable
- Difficulty is in establishing trust
  - 20% technology – 80% policy

Questions



Answers: **http://www.pki-page.org/**
http://www.rsasecurity.com/rsalabs/faq/
http://csrc.nist.gov/pki/
Planning for PKI, Russ Housley and Tim I
John Wiley & Sons, Inc. 2001